

CLAIMS

What is claimed is:

5

1. A method for access management in a distributed data processing system, the method comprising:

10 receiving from a client a request to access a resource protected by an application service provider (ASP) aggregator service, wherein the ASP aggregator service provides single-sign-on functionality for a plurality of net-sourced applications, wherein at least one of the net-sourced applications is hosted by an ASP;

15 in response to a determination that the client or a user of the client has not been properly authenticated by the ASP aggregator service for a current client session, requiring the client or the user of the client to successfully complete an authentication process; and

20 sending to the client a response to the request received from the client, wherein the response is accompanied by an aggregator token, wherein the aggregator token comprises a logon resource identifier.

25 2. The method of claim 1 wherein a logon resource identified by the logon resource identifier prompts the client or a user of the client to complete an authentication operation.

30 3. The method of claim 1 wherein the logon resource identifier is a Uniform Resource Identifier (URI).

4. The method of claim 3 wherein the logon resource identifier is a Uniform Resource Locator, and the logon resource is a logon Web page.

5 5. The method of claim 1 further comprising:

receiving from the client a request to access a net-sourced application hosted by an ASP;

10 extracting a logon resource identifier from an aggregator token that accompanies the request, wherein the aggregator token originated from the ASP aggregator service, wherein the ASP aggregator service provides single-sign-on functionality for a plurality of net-sourced applications, wherein at least one of the net-sourced applications is the net-sourced application
15 hosted by the ASP; and

sending to the client a response indicating the logon resource identifier as a redirectable destination.

6. A method for access management in a distributed data processing system, the method comprising:

receiving from a client a request to access a net-sourced application hosted by an application service provider (ASP);

extracting a logon resource identifier from an aggregator token that accompanies the request, wherein the aggregator token originated from an ASP aggregator service, wherein the ASP aggregator service provides single-sign-on functionality for a plurality of net-sourced applications, wherein at least one of the net-sourced applications is the net-sourced application hosted by the ASP; and

sending to the client a response indicating the logon resource identifier as a redirectable destination.

7. The method of claim 6 further comprising:

determining that the client or a user of the client has not been properly authenticated prior to sending the response to the client.

8. The method of claim 7 further comprising:

determining that the request was not accompanied with a valid application authentication token.

9. The method of claim 6 wherein access for the client to the net-sourced application is controlled by the ASP on a subscription basis.

10. The method of claim 6 wherein a logon resource identified by the logon resource identifier prompts the client or a user of the client to complete an authentication operation.

5

11. The method of claim 6 wherein the logon resource identifier is a Uniform Resource Identifier (URI).

12. The method of claim 11 wherein the logon resource
10 identifier is a Uniform Resource Locator, and the logon
resource is a logon Web page.

13. A method for access management in a distributed data processing system, the method comprising:

receiving from a client a request to access a logon resource identified by a logon resource identifier that
5 has been extracted from an aggregator token, wherein access to the logon resource is protected by an application service provider (ASP) aggregator service, wherein the ASP aggregator service provides
single-sign-on functionality for a plurality of
10 net-sourced applications;

requiring the client or the user of the client to successfully complete an authentication process associated with the logon resource;

extracting an origination identifier from the
15 request, wherein the origination identifier identifies a net-sourced application that is one of the plurality of net-sourced applications; and

sending a response to the client, wherein the response indicates the origination identifier as a
20 redirectable destination.

14. The method of claim 13 wherein the logon resource identifier is a Uniform Resource Identifier (URI).

25 15. The method of claim 14 wherein the logon resource identifier is a Uniform Resource Locator, and the logon resource is a logon Web page.

16. An apparatus for access management in a distributed data processing system, the apparatus comprising:

means for receiving from a client a request to access a resource protected by an application service provider (ASP) aggregator service, wherein the ASP aggregator service provides single-sign-on functionality for a plurality of net-sourced applications, wherein at least one of the net-sourced applications is hosted by an ASP;

means for requiring the client or the user of the client to successfully complete an authentication process in response to a determination that the client or a user of the client has not been properly authenticated by the ASP aggregator service for a current client session; and

means for sending to the client a response to the request received from the client, wherein the response is accompanied by an aggregator token, wherein the aggregator token comprises a logon resource identifier.

17. The apparatus of claim 16 wherein a logon resource identified by the logon resource identifier prompts the client or a user of the client to complete an authentication operation.

18. The apparatus of claim 16 wherein the logon resource identifier is a Uniform Resource Identifier (URI).

19. The apparatus of claim 18 wherein the logon resource identifier is a Uniform Resource Locator, and the logon resource is a logon Web page.

20. The apparatus of claim 16 further comprising:

means for receiving from the client a request to
access a net-sourced application hosted by an ASP;

means for extracting a logon resource identifier
5 from an aggregator token that accompanies the request,
wherein the aggregator token originated from the ASP
aggregator service, wherein the ASP aggregator service
provides single-sign-on functionality for a plurality of
net-sourced applications, wherein at least one of the
10 net-sourced applications is the net-sourced application
hosted by the ASP; and

means for sending to the client a response
indicating the logon resource identifier as a
redirectable destination.

15

21. An apparatus for access management in a distributed data processing system, the apparatus comprising:

means for receiving from a client a request to access a net-sourced application hosted by an application service provider (ASP);

means for extracting a logon resource identifier from an aggregator token that accompanies the request, wherein the aggregator token originated from an ASP aggregator service, wherein the ASP aggregator service provides single-sign-on functionality for a plurality of net-sourced applications, wherein at least one of the net-sourced applications is the net-sourced application hosted by the ASP; and

means for sending to the client a response indicating the logon resource identifier as a redirectable destination.

22. The apparatus of claim 21 further comprising:

means for determining that the client or a user of the client has not been properly authenticated prior to sending the response to the client.

23. The apparatus of claim 22 further comprising:

means for determining that the request was not accompanied with a valid application authentication token.

24. The apparatus of claim 21 wherein access for the client to the net-sourced application is controlled by the ASP on a subscription basis.

25. The apparatus of claim 21 wherein a logon resource identified by the logon resource identifier prompts the client or a user of the client to complete an authentication operation.

5

26. The apparatus of claim 21 wherein the logon resource identifier is a Uniform Resource Identifier (URI).

10

27. The apparatus of claim 26 wherein the logon resource identifier is a Uniform Resource Locator, and the logon resource is a logon Web page.

11/20/2009 10:00:00 AM

28. An apparatus for access management in a distributed data processing system, the apparatus comprising:

means for receiving from a client a request to access a logon resource identified by a logon resource identifier that has been extracted from an aggregator token, wherein access to the logon resource is protected by an application service provider (ASP) aggregator service, wherein the ASP aggregator service provides single-sign-on functionality for a plurality of net-sourced applications;

means for requiring the client or the user of the client to successfully complete an authentication process associated with the logon resource;

means for extracting an origination identifier from the request, wherein the origination identifier identifies a net-sourced application that is one of the plurality of net-sourced applications; and

means for sending a response to the client, wherein the response indicates the origination identifier as a redirectable destination.

29. The apparatus of claim 28 wherein the logon resource identifier is a Uniform Resource Identifier (URI).

30. The apparatus of claim 29 wherein the logon resource identifier is a Uniform Resource Locator, and the logon resource is a logon Web page.

31. A computer program product in a computer readable medium for use in a distributed data processing system for managing access to resources, the computer program product comprising:

5 instructions for receiving from a client a request to access a resource protected by an application service provider (ASP) aggregator service, wherein the ASP aggregator service provides single-sign-on functionality for a plurality of net-sourced applications, wherein at
10 least one of the net-sourced applications is hosted by an ASP;

instructions for requiring the client or the user of the client to successfully complete an authentication process in response to a determination that the client or
15 a user of the client has not been properly authenticated by the ASP aggregator service for a current client session; and

instructions for sending to the client a response to the request received from the client, wherein the
20 response is accompanied by an aggregator token, wherein the aggregator token comprises a logon resource identifier.

32. The computer program product of claim 31 wherein a
25 logon resource identified by the logon resource identifier prompts the client or a user of the client to complete an authentication operation.

33. The computer program product of claim 31 wherein the
30 logon resource identifier is a Uniform Resource Locator, and the logon resource is a logon Web page.

34. The computer program product of claim 31 further comprising:

instructions for receiving from a client a request
5 to access a net-sourced application hosted by an ASP;

instructions for extracting a logon resource
identifier from an aggregator token that accompanies the
request, wherein the aggregator token originated from an
ASP aggregator service, wherein the ASP aggregator
10 service provides single-sign-on functionality for a
plurality of net-sourced applications, wherein at least
one of the net-sourced applications is the net-sourced
application hosted by the ASP; and

instructions for sending to the client a response
15 indicating the logon resource identifier as a
redirectable destination.

35. A computer program product in a computer readable medium for use in a distributed data processing system for managing access to resources, the computer program product comprising:

5 instructions for receiving from a client a request to access a net-sourced application hosted by an application service provider (ASP);

10 instructions for extracting a logon resource identifier from an aggregator token that accompanies the request, wherein the aggregator token originated from an ASP aggregator service, wherein the ASP aggregator service provides single-sign-on functionality for a plurality of net-sourced applications, wherein at least one of the net-sourced applications is the net-sourced application hosted by the ASP; and

15 instructions for sending to the client a response indicating the logon resource identifier as a redirectable destination.

20 36. The computer program product of claim 35 further comprising:

25 instructions for determining that the client or a user of the client has not been properly authenticated prior to sending the response to the client.

37. The computer program product of claim 36 further comprising:

30 instructions for determining that the request was not accompanied with a valid application authentication token.

38. A computer program product in a computer readable medium for use in a distributed data processing system for managing access to resources, the computer program product comprising:

5 instructions for receiving from a client a request to access a logon resource identified by a logon resource identifier that has been extracted from an aggregator token, wherein access to the logon resource is protected by an application service provider (ASP) aggregator
10 service, wherein the ASP aggregator service provides single-sign-on functionality for a plurality of net-sourced applications;

15 instructions for requiring the client or the user of the client to successfully complete an authentication process associated with the logon resource;

20 instructions for extracting an origination identifier from the request, wherein the origination identifier identifies a net-sourced application that is one of the plurality of net-sourced applications; and

 instructions for sending a response to the client, wherein the response indicates the origination identifier as a redirectable destination.